International Journal of Electrical Engineering and Technology (IJEET)
Volume 12, Issue 11, November 2021, pp. 97-109, Article ID: IJEET_12_11_009
Available online at https://iaeme.com/Home/issue/IJEET?Volume=12&Issue=11
ISSN Print: 0976-6545 and ISSN Online: 0976-6553
DOI: https://doi.org/10.34218/IJEET.12.11.2021.009

A DECISION-MAKING MODEL FOR REINFORCING A CORPORATE INFORMATION SECURITY SYSTEM

Yong-Ho Kim[1], Bo-Young Kim[2]
[1,2]Seoul Business School, aSSIST University, 46, Ewhayeodae 2gil, Seodaemungu, Seoul, South Korea

ABSTRACT

Recently, information security incidents such as personal information leakage have been regarded as serious risk factors that directly affect corporate sales reduction and corporate image loss. In order to manage information security systematically, enterprises have been introducing information security systems more than ever before. This study aims to derive major items of the information security system mainly for corporate organizational management, with a focus on the technology-organization-environment (TOE) framework, and suggests a direction for system build-up and management. To this end, the Analytic Hierarchy Process (AHP) was conducted on 20 items derived from previous studies. A survey was conducted among 24 individuals, including 12 corporate internal administrators and 12 corporate external consultants. As a result, it turned out that environmental factors affected the information security system more significantly among technical, organizational, and environmental factors. Notably, 'compliance with legal requirements,' 'protection of information subjects' rights,' and 'increase of the information security awareness' affected the operation of the information security system or related decision-making processes. This finding suggests that although technical and organizational management is also essential when it comes to corporate information security system operation, the system needs to respond swiftly to rapid market changes and legal and administrative changes concerning information security.

Key words: Information security, TOE framework, Decision-making model, AHP.

Cite this Article: Yong-Ho Kim and Bo-Young Kim, A Decision-Making Model for Reinforcing a Corporate Information Security System, *International Journal of Electrical Engineering and Technology (IJEET).* 12(11), 2021, pp. 97-109. https://iaeme.com/Home/issue/IJEET?Volume=12&Issue=11

1. INTRODUCTION

As the 3rd Industrial Revolution based on corporate economic activity and information through the Internet and computers led to the 4th Industrial Revolution, key technologies have expanded throughout the industry. Particularly with the rapid advancement of key technologies of the 4th Industrial Revolution such as IoT, Cloud, Big Data, Mobile 5G, AI, Blockchain, 3D Printing, and Robotics [1], a wide range of technology areas are used in various corporate information management areas such as information collection, storing, and utilization. While such technologies help maximize the ripple effect on corporate economic activity, threats to information security are also involved, including information capture, interference, and misuse [2].

Many enterprises around the globe have reported losses from information security vulnerabilities. For example, a large financial holding company called Capital One in the U.S. involved a mistake in cloud service settings in 2019, leading to a customer information leakage involving 160,000,000 individuals. In 2020, updates to Orion of SolarWinds, a universal IT management software program in the U.S., included a malicious code of a value-chain attack type that invaded 18,000 enterprises around the globe. Recently, such intrusions were spread through VPNs commonly used among those working from home in response to such national disasters as COVID-19, and even channels viewed as secure and reliable were not exempted from large-scale security incidents. After all, as the technology advancement accelerates, the necessity of general inspection on the corporate information security system and general plans to strengthen the information security is more emphasized [3].

Indeed, information security is one of the most critical business management elements. One security incident is a severe threat that may lead to customer separation, sales decrease, and loss of the corporate image. Moreover, corporate awareness on the importance of information security has increased in line with social changes. The number of enterprises introducing an information security system to manage information security systematically is increasing. Particularly, to secure corporate business continuity and efficiently cope with information leakage attempts that are more intelligent than their precedents, it is vital to build and manage information security in a manner more systematic than the existing product-centered technical response [4].

Most previous studies, however, focused on comparing the importance of each specific item of the ISMS that is the basis for corporate information security checkup and planning [5] or technical activity for information security, specifically on such items as an investment into information security and incident control [6]. As the range of corporate information security is extended, it is necessary to build an information security system connected with major business strategies in digital environments. Thus, it is vital to examine corporate information security systems and management methods [7].

Accordingly, this study defines primary considerations for reinforcing the corporate information security system in terms of organization, technology, and environment, based on the TOE framework. In addition, significant factors that affect the efficiency of a corporate information security system most significantly are derived in this study. This study presents specific implications that help good and efficient decision-making regarding corporate information security system build-up and management.

2. LITERATURE REVIEW

2.1. Corporate Information Security System

"Information security" means to build administrative and technical means to prevent damage, alteration, and leakage of information in the process of information collection, processing, storing, searching, and transmission. The information security system is a type of administrative and technical means in this regard. The 'Information Security Management System (ISMS)' involves a series of steps and activities to systematically and continually build, document, manage, and operate information security procedures and steps so that the primary goals of information security—confidentiality, integrity, and information asset availability—are fulfilled [8] . In addition, the ISMS certification system, through which a third-party certification institution evaluates the information security being operated in an organization objectively and independently, thus guarantees standards fulfillment.

Corporate information security activity includes risk management and information security measures throughout administrative, technical, and physical security sectors mainly based on Information Security Management System (ISMS) standards. The ISMS is a basis for the systematic build-up and continued control and operation of corporate information asset management procedures and steps to secure confidentiality, integrity, and availability. In order to check corporate safety and reliability, the official review is conducted by independent institutions such as the Korea Internet and Security Agency designated by the Korea Communications Commission based on the certification criteria [9].

Information security systems currently applicable at home and abroad include the following: Information Security Management Systems Requirements (ISO27001), Managing Risk from Information Systems from An Organizational Perspective (NIST SP800-39), Korea Internet and Security Agency Information Security Management System (KISA ISMS), Personal Information Management System (PIMS), Government-Information Security Management System (G-ISMS), Information Security Check Service, information (ISCS), and Critical Information Infrastructure Protection (CIIP) [10].

In Korea, in order to reduce confusion among institutions concerned, as well as burdens on the use of resources due to the similarity and separate operation of regulatory items of the PIMS and ISMS after the Personal Information Protection Act came into effect, the ISMS and PIMS were integrated into the ISMS-P on November 7, 2018. Regulatory items of each management system are as follows Table 1.

Table 1 Certification criteria of information security and personal Information Security Management Systems

Area (No. of items)	Sector (No. of sub-items)	Applicability	
		ISMS	ISMS-P
1. Build-up and operation of the management system (16)	1.1. Build-up of the framework for the management system (6)	O	O
	1.2. Risk management (4)	O	O
	1.3. Operation of the management system (3)	O	O
	1.4. Checkup and improvement of the management system (3)	O	O
2. Requirements for protective measures (64)	2.1. Policy, organization, and asset management (3)	O	O
	2.2. Personnel security (6)	O	O
	2.3. Visitor security (4)	O	O
	2.4. Physical security (7)	O	O
	2.5. Authentication and authorization management (6)	O	O
	2.6. Access control (7)	O	O
	2.7. Encryption (2)	O	O

	2.8. Information system implementation, development, and security (6)	O	O
	2.9. System/service operation and management (7)	O	O
	2.10. System/service security management (9)	O	O
	2.11. Incident prevention and response (5)	O	O
	2.12. Disaster recovery (2)	O	O
3. Requirements for each step of personal information processing (22)	3.1. Protective measures for personal information collection (7)		O
	3.2. Protective measures for personal information retention and use (5)		O
	3.3. Protective measures for personal information provision (4)		O
	3.4. Protective measures for personal information destruction (3)		O
	3.5. Protection of the information object's rights (3)		O

Source: KISA. January 2019

Such rapid changes in IT convergence environments have raised keen awareness on threats to and vulnerability of information assets such as personal information and corporate information and, accordingly, appropriate risk management activities are necessary [11]. To protect such corporate information assets and strengthen organizational competitiveness, efforts have been put forth continually to build and operate an Information Security Management System to enhance the information security management process. The value of information assets is an essential element that decides the development and continuity of an organization, whereas the proper operation of a consistent, systematic, and comprehensive Information Security Management System for significant information assets is essential to minimize the organization's loss, secure a competitive edge, and thus improve the reliability and value of the organization.

For this reason, the importance of information security governance has been recently emphasized [12]. According to the business objective, an enterprise's information security activity is the beginning of governance to build and operate information security goals. The operation, control, and continued monitoring of the information security system [13] is the very basis to create synergy effects in business strategies and organizational decision making.

2.2. The Effect Factors of a Corporate Information Security System

Information security system frameworks being applied and operated at home and abroad present measurement items for information security circulation models and performance (see Table 2).

Table 2 Classification of information security performance measurements for each framework of the information security systems

Framework	Classification of information security performance measurements
BCMM	- Improvement of information security awareness (among executives and employees) - Level of information asset control (resources provided)
ISM3	- Level of access setting (access control) - Integrated security applicability (development security)
ISO27004	- Level of compliance with legal requirements (legal compliance, security audit, law and agreement, administration system efficiency) - Level of risk management and response (business risk, risk assessment, treatment, and input/output management) - Improvement of information security awareness (education on the management system efficiency) - Sales increase (economic performance and sales increase) - Cost-saving (economic performance and cost-saving) - Image improvement (organizational value increase)
JIPDEC	- Level of compliance with legal requirements (internal audit and law compliance)

	- Improvement of information security awareness (improvement of the brand recognition and security level improvement) - Work satisfaction (productivity improvement)
KISA	- Applicability of integrated security measures (system and data protection, and information security base index) - Work satisfaction (work efficiency) - Rate of proper measures for infringement incidents such as malware invasion (infringement by hacking or viruses, and privacy infringement)
NIST SP800-55	- Applicability of integrated security (determination on the level of embodiment of information security programs, and an embodiment of information security programs)

As a prominent example, the ISMS-P is a series of steps and activities to document information security steps, including personal information systemically, and to manage and operate such steps continually and efficiently. With such steps and activities, ISMS-P aims to realize the confidentiality, integrity, and availability of information assets. This way, it is possible to improve business stability and secure legal compliance regarding information security for ethical and transparent business management. In addition, ISMS-P-certified organizations can minimize financial losses even in incidents of infringement or class suits [9, 13].

As examples of previous studies emphasizing the value of information security systems in business management, Eloff and Eloff [14] viewed, as essential factors, compliance with legal requirements, risk management, and response, and information security awareness. Posthumus and Von Solms [15] is also viewed as necessary, compliance with legal requirements, auditing, monitoring, access setting, and measures for infringement incidents such as malware invasion. Richards [16] emphasized risk management and response as the most crucial element, presenting sub-factors such as risk management activity, risk analysis, and risk identification. In addition, Von Solms [17] suggested improving information security awareness through education and maintenance and control of information security activity as vital factors. Bulgurcu et al. [18] pointed out the importance of compliance with legal requirements, information asset control system, maintenance, control, access setting, and integrated security applicability.

Such factors may be explained with the TOE framework that Witty and Hallawell, [19]. suggested classifying elements affected in the process of an organization's introduction and management of information technology. As stated in previous studies [8, 20], factors affecting the information security system may be derived based on the three factors: environment, technology, and organization. First of all, the external environmental context means the area of activity where an enterprise runs its business. The industry sector that the enterprise belongs to, the enterprise's competitors, resource suppliers, and the government are part of the external environmental context. The technical context includes all the technologies in and out of the organization that it faces. This means not only technologies inside the organization but also every other technology available in the market. Finally, the organizational context means the organization's characteristics. In general, an organization's characteristics include its scale, centralization, formulation, complexity, human resource quality, and extra internal resources.

3. RESEARCH METHODS

3.1. Analytic Hierarchy Process (AHP)

The Analytic Hierarchy Process (AHP) is a method used to select one solution in a situation where various purposes are essential to the decision-maker. The relative importance of different alternatives is compared and quantified to evaluate them and solve a complicated problem. If there are multiple and complex goals or evaluation criteria of decision-making, this method

may be used to support the systematic evaluation of mutually exclusive alternatives. Attributes of a problem are examined systematically and hierarchically to standardize them [21].

Early in the 1970s, in collaborative work with game theory experts and Professor Thomas Saaty, this method was developed as an alternative to address the inefficiency of decision-making processes [22]. This is a decision-making methodology to detect the evaluator's knowledge, experience, and intuition by way of pairwise comparison between elements that form the decision-making hierarchy. The AHP is widely utilized to derive key factors, set policy alternatives, and establish strategies [23]. The AHP methodology derives the evaluation results based on the total ranks of relative importance among elements determined by each evaluator [24]. Accordingly, this study utilizes the AHP in evaluating the relative importance of significant factors that affect the reselling of limited-edition products.

Between the two AHP analysis approaches, the 'geometric mean of pairwise comparison' was used to calculate the relative importance. This method is widely used and determines the relative importance of factors based on the geometric average of each element. Considering probabilistic characteristics based on which the difference between an input variable and a model output variable are examined, it was sought to secure the reliability of calculation bases and results of input variables by setting the weight of each factor. To this end, the analysis was conducted employing the AHP variable weight calculation method suggested by Gangwar et al. [25].

3.2. Research Framework and Variables

Based on previous studies, this study sets and comparatively analyzes 'technical factors,' 'organizational factors,' and 'environmental factors' based on the TOE framework as determinants of decision-making to reinforce corporate information security management. 'Technical factors' mean technology-related factors that affect decision-making on activities to strengthen information security such as information collection and management, information access control, cyber damage recovery, response to information security threats, information asset control, application of integrated security technology, etc.

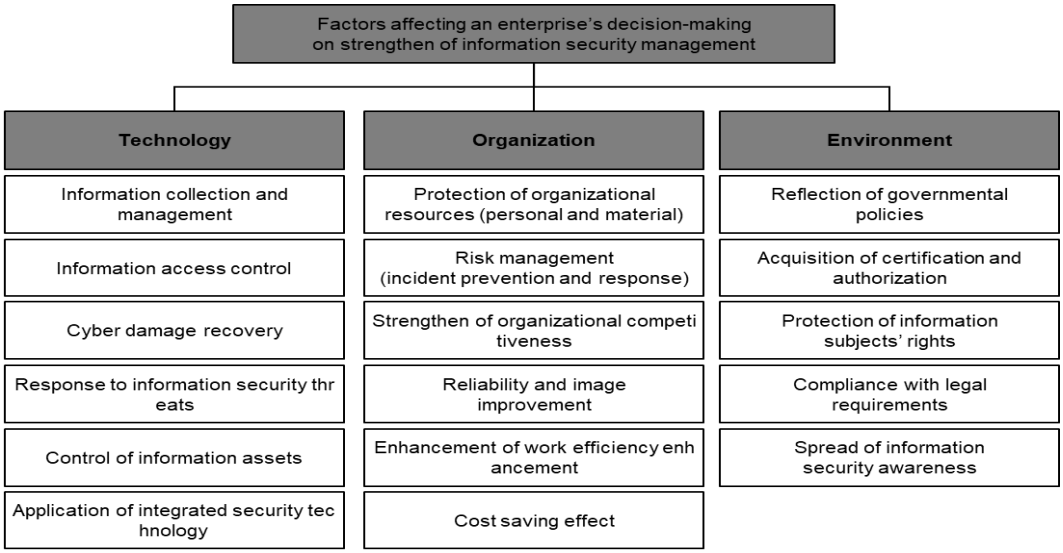

Figure 1 Research Framework

'Organizational factors' mean the factors that affect organizational aspects regarding activities to strengthen information security, such as organizational resource protection, risk management, reinforcing of organizational competitiveness, reliability and image improvement, work efficiency enhancement, and cost-saving effect. Finally, 'environmental

factors' include both policy environment factors such as reflection of governmental policies, acquisition of certification or authorization, compliance with legal requirements, and factors that affect market environments such as protection of information subjects' rights and spread of information security awareness (see Figure 2). Three key variables consisting of 20 components in total listed above (See Table 3).

Table 3 Evaluation factors and definition

Evaluation Area	Evaluation Factors	Factor Definition	Related References
Technology	Information collection and management	It is thought that activities to manage information security should be strengthened because information collection and management are important.	Jeyaraj et al. [26] Kamal [27], Al-Natour and Benbasat [28], Hossain and Quaddus [29]
	Information access control	It is thought that activities to manage information security should be strengthened because information access control is valuable.	
	Cyber damage recovery	It is thought that activities to manage information security should be strengthened because cyber damage recovery is of importance.	
	Response to information security threats	It is thought that activities to manage information security should be strengthened because a proper response to information security threats is essential.	
	Information asset control	It is thought that activities to manage information security should be strengthened because information asset control is vital.	
	Application of integrated security technology	It is thought that activities to manage information security should be strengthened because application of integrated security technology is of crucial.	
Organization	Organizational resource protection	It is thought that activities to manage information security should be strengthened because they would be helpful for the protection of human, material, and organizational resources.	Ajzen [30], Alsene [31], Grandon and Pearson [32]
	Risk management	It is thought that activities to manage information security should be strengthened because they would be helpful for organizational risk management.	
	Reinforcing of organizational competitiveness	It is thought that activities to manage information security should be strengthened because they would help reinforce organizational competitiveness.	
	Reliability and image improvement	It is thought that activities to manage information security should be strengthened because they would be helpful for reliability and image improvement.	
	Work efficiency enhancement	It is thought that activities to manage information security should be strengthened because they would be helpful for work efficiency enhancement.	
	Cost-saving effect	It is thought that activities to manage information security should be strengthened because they would be helpful for cost-saving.	
Environment	Reflection of governmental policies	It is thought that activities to manage information security should be strengthened in order to reflect governmental policies.	Davis [33], Caldeira and Ward [34], Eze et al. [35]
	Acquisition of certification or authorization	It is thought that activities to manage information security should be strengthened to acquire certification or authorization.	
	Protection of information subjects' rights	It is thought that activities to manage information security should be strengthened to protect information subjects' rights (customers and those interested in the business).	
	Compliance with legal requirements	It is thought that activities to manage information security should be strengthened to comply with legal requirements.	
	Spread of information security awareness	It is thought that activities to manage information security should be strengthened in line with the spread of information security awareness.	

3.3. Research Process and Data Collection

This study analyzes factors affecting consumers' activities of limited-edition product reselling. To this end, a pairwise comparison questionnaire was utilized in applying the AHP methodology and based on the research framework shown in Figure 1. The questionnaire consists of 44 questions: 1 subjective question and 43 multiple choice questions of a pairwise comparison scale. A pilot test was conducted among five experts in the area of information security.

Individuals selected for the survey were experts with a deep understanding of corporate information security activities and currently handling related duties. However, it should be noted that corporate information security activities are classified into two classes: those promoted by an enterprise with its independent team; and those promoted by an external consulting agency. In consideration of such aspects, the survey was conducted among consultants from external consulting agencies that help strengthen the enterprise's information security activities and information security administrators in an enterprise. In consideration of the expertise and experience, survey subjects were selected among individuals with about 10 years of experience in the industry.

The survey was conducted for 1 month in December 2020 by way of one-to-one interviews. The survey background and definitions of variables were explained to each of the survey participants for at least 1 hour to understand them fully. They answered the survey questions based on the detailed guideline of the researcher. 24 questionnaires were collected from 12 corporate internal administrators and 12 corporate external consultants and then analyzed.

4. RESULTS

4.1. Comparison of Evaluation Variables

The consistency ratio (CR) was all under 0.2659, which was significant. As shown in Table 4 regarding factor analysis results, 3 key factor groups affecting the improvement of corporate information security management were in the order of environmental factors (0.484), organizational factors (0.329), and technical factors (0.188). Thus, it turned out that the most influential factors on decision-making on information security management activity were environmental factors. Specifically, compliance with legal requirements (0.131) was the most influential subfactor. The importance of the other sub-factors was in the order of protection of information on subject rights (0.128), risk management (0.095), and reflection of governmental policies (0.089). In addition, factors of market environments such as protection of organizational resources (0.081) and spread of information security awareness (0.081) also turned out to be necessary, influential factors.

Table 4 Weights and priority of evaluation variables

Evaluation areas	The weights of areas	Evaluation factors	The weights of evaluation factors			
	Local		Local	Priority	Global	Priority
Technology	0.188	Information collection and Management	0.132	4	0.025	13
		Information access control	0.221	2	0.041	10
		Cyber damage recovery	0.085	6	0.016	16
		Response to information security threats	0.229	1	0.043	9
		Information asset control	0.206	3	0.039	11
		Application of integrated security technology	0.127	5	0.024	14
Organization	0.329	Organizational resource protection	0.248	2	0.081	5

		Risk management	0.290	1	0.095	3
		Reinforcing of organizational competitiveness	0.151	4	0.049	8
		Reliability and image improvement	0.171	3	0.056	5
		Work efficiency enhancement	0.087	5	0.029	12
		Cost saving effect	0.053	6	0.017	15
Environment	0.484	Reflection of governmental policies	0.185	3	0.089	4
		Acquisition of certification or authorization	0.112	5	0.054	7
		Protection of information subjects' rights	0.265	2	0.128	2
		Compliance with legal requirements	0.271	1	0.131	1
		Spread of information security awareness	0.168	4	0.081	5
Total	1.0000		3.000		1.0000	

4.2. Comparison of Evaluation Areas between Expert and Reseller Groups

As the corporate internal manager group was compared with the consulting expert group, the results turned out to be the same. As shown in Table 5, the weight of factors was in the order of environment, organization, and technology in both groups. However, the corporate internal administrator group turned out to view more critical environmental factors (0.484) and technical factors (0.212) than the other. The consulting expert group turned out to view, as more important, organization factors (0.354).

Table 5 Comparison analysis results on evaluation areas

Evaluation areas	**The weights of areas**			
	Corporate Inner Group		**Consulting Group**	
	Local	**Priority**	**Local**	**Priority**
Environment	0.484	1	0.477	1
Organization	0.305	2	0.354	2
Technology	0.212	3	0.169	3
Total	1.0000		1.0000	

4.3. Comparison of Evaluation Factors between Expert and Reseller Groups

As shown in Table 6, the comparative analysis of specific factors between the groups indicates that the most important influential factor in both groups was 'compliance with legal requirements and then 'protection of information subjects' rights' followed. In the comparative analysis of the 3rd to 6th factors, it turned out that 'reflection of governmental policies' was the third in the case of the corporate internal administrator group (0.094) and the sixth in the case of the consulting group (0.083).

Thus, this factor was regarded as far more important by the corporate internal administrator group. The 'risk management factor' was the fourth in the case of the corporate internal management group (0.090) and the third in the case of the consulting group (0.100). Thus, this factor was regarded as more important by the consulting group. 'Spread of information security awareness' was the fifth in both cases of the corporate internal management group (0.077) and the consulting group (0.084). Finally, the factor of 'protection of organizational resources' was the sixth in the case of the corporate internal management group (0.070) and the fourth in the case of the consulting group (0.094). Thus, it turned out that the consulting group was more affected by this factor than the corporate internal management group.

Table 6 Comparison analysis results on evaluation factors

Evaluation factors	The weights of evaluation factors				Priority of factors (Global)	
	Local		Global			
	Corporate Inner Group	Consulting Group	Corporate Inner Group	Consulting Group	Corporate Inner Group	Consulting Group
Information collection and management	0.139	0.123	0.029	0.021	14	15
Information access control	0.231	0.209	0.049	0.035	8	11
Cyber damage recovery	0.081	0.090	0.017	0.015	17	17
Response to information security threats	0.250	0.209	0.053	0.035	7	10
Information asset control	0.201	0.208	0.043	0.035	12	11
Application of integrated security technology	0.098	0.161	0.021	0.027	15	13
Organizational resource protection	0.230	0.265	0.070	0.094	6	4
Risk management	0.295	0.283	0.090	0.100	4	3
Reinforcement of organizational competitiveness	0.154	0.146	0.047	0.052	11	9
Reliability and image improvement	0.158	0.186	0.048	0.066	10	7
Work efficiency enhancement	0.103	0.073	0.031	0.026	13	14
Cost saving effect	0.061	0.047	0.019	0.017	16	16
Reflection of governmental policies	0.194	0.175	0.094	0.083	3	6
Acquisition of certification or authorization	0.101	0.124	0.049	0.059	8	8
Protection of information subjects' rights	0.272	0.255	0.132	0.122	2	2
Compliance with legal requirements	0.274	0.270	0.133	0.129	1	1
Spread of information security awareness	0.159	0.176	0.077	0.084	5	5
	3.000	3.000	1.0000	1.0000		

5. CONCLUSION

Based on previous studies, this study comparatively analyzes significant factors related to reinforcing the corporate information security system, focusing on technology, organization, and environmental factors. As a result, significant factors affecting decision-making were derived. Three major findings derived from this study may be summarized below: First, it turned out that the environmental factor was the most important among the three factors affecting corporate information security management. Mainly, compliance with legal

requirements was the most crucial subfactor. This result aligned with the related previous studies in compliance with legal requirements.

Above all, differences in information security experts' awareness of the importance and current conditions of system management such as scale depend on the internal political perspectives and external regulations rather than experts' opinions on information security. Because of these characteristics, it is necessary to reconsider the status and decision-making authority of information security experts within an enterprise. As for information security experts, it is necessary to improve the ability to solve administrative problems related to political and regulatory environment factors and technical problems.

Second, both the corporate internal administrator and information security consulting expert groups viewed environment and organization factors as more important than technology. Traditionally, regarding the build-up and management of an information security system, important topics in guidelines or frameworks for information security regulation were technical factors such as information collection, information control, and threat management in terms of regulatory management. For this reason, such technology-centered discussion has limitations in that it focuses on the information security system itself while organizational synergy and systematic strategies within the enterprise are often neglected.

As stated in the findings of this study, however, the corporate information security system considers awareness in and out of the organization and compliance with regulations regarding information management in such aspects as the spread of information security awareness and protection of information subjects' rights. In addition, it is emphasized that there should be organizational responses to risks in terms of the protection of organizational resources. In other words, an enterprise's information security system should be built as a systematic operation mechanism that considers its vision, the direction of strategies, and governance, not merely to solve technical management problems.

Finally, major influential factors regarding the information security system were almost the same between the corporate internal administrator group of information security and the consulting expert group. This means that there is little difference in the goals and direction of information security system management operations in and out of an organization. In the past, access control was practiced, focusing on personnel security since the primary cause of information leakage was an insider. For this reason, the access control focused on an unauthorized outsider (information security consultant). However, as it is easier for an insider to access a significant system compared to an outsider, the priority should be given to management and investment into insiders' access control. When it comes to internalizing information assets, strengthening control or management over an enterprise's insiders rather than outsiders to improve the system operation's effectiveness, is recommended.

However, this study has the following limitations: First, 20 factors affecting the information security system were derived based on the TOE framework. On the other hand, this study does not reflect factors to be considered to build a system for cooperative strategies or business strategies in the context of corporate information security activity. Future studies need to derive and add influential factors to consider interactions between recent corporate information security system characteristics and business management activities. Second, this study does not consider business types or scales.

When an information security system is introduced and operated in an organization, its characteristics may depend on the business type or scale. Thus, it is necessary to consider and comparatively analyze the business type and scale more thoroughly. Finally, this study was conducted among information security experts in Korea. For this reason, the generalization of its findings has limitations. Future studies may include experts from global enterprises. In

addition, empirical research on whether such influential factors significantly impact an enterprise's actual information security performance or result also needs to be conducted.

REFERENCES

[1] J. Bloem, M. Van Doorn, S. Duivestein, D. Excoffier, R.Maas, E. Van Ommeren, The Fourth industrial revolution (*Things Tighten*, 2014).

[2] C. Vroom, and R. von Solms, Towards information security behavioural compliance, *Computers & Security*, 23(3), 2004, 191-198.

[3] A. Wiley, A, McCormac, and D. Calic, More than the individual: Examining the relationship between culture and Information Security Awareness, *Computers & Security*, 88, 2020, 101640.

[4] A. Martins, and J. H. P. Eloff, Information security culture (*Boston: Kluwer Academic Publishers*, 2002).

[5] S. Jeong, J. Yoon, J. Lim, and K. Lee, Studies on the effect of information security investment executive, *Journal of the Korea Institute of Information Security & Cryptology*, 24(6), 2014, 1271–1284.

[6] H. Henriksen, Motivators for IOS adoption in Denmark, *Journal of Electronic Commerce in Organizations*, 4(2), 2006, 25-39.

[7] W. N. Choi, W. J. Kim, and K. H. K. Kook, An evaluation of the efficiency of information protection activities of private companies, *Convergence Security Journal*, 18(5), 2018, 25–32.

[8] L. Barnard, and R. Von Solms, A formalized approach to the effective selection and evaluation of information security controls, *Computers & Security*, 19(2), 2000, 185-194.

[9] A. Da Veiga, and J. H. P. Eloff, An information security governance framework, *Information Systems Management*, 24(4), 2007, 361-372

[10] H. Lee, and S. Chai, An empirical study of relationship between information security investment and information security incidents, *Journal of the Korea Institute of Information Security & Cryptology*, 28(1), 2018, 269–281.

[11] Y. C. Kang, and J. C. Ahn, A study on primary control area for information security management system: Focusing on the domestic three industries, *The Journal of Korea Academy Industrial Cooperation Society*, 2021, 22(4), 140–149.

[12] Z. A. Soomro, M. H. Shah, J. Ahmed, Information security management needs more holistic approach: A literature review, *International Journal of Information Management*, 36(2), 2016, 215-225.

[13] C. Lee, J. Kim, and C. Lee, A comparative study on the priorities between perceived importance and investment of the areas for information security management system, *Journal of the Korea Institute of Information Security & Cryptology*, 24(5), 2014, 919–929.

[14] J. H. P. Eloff, and M. Eloff, Integrated Information Security Architecture, *Computer Fraud and Security*, 11(1), 2005, 10–16

[15] S. Posthumus, and R. Von Solms, IT governance, *Computer Fraud and Security*, 6(1), 2005, 11–17.

[16] N. Richards, The critical importance of information security to financial institutions, *Business Credit*, 104(9), 2002, 35–36.

[17] B. Von Solms, Information security—The third wave?, *Computers and Security*, 19(7), 2000, 615–620.

[18] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly*, 24(3), 2010, 523-548

[19] R. J. Witty, and A. Hallawell, (2003). Client issues for security policies and architecture (Gartner, 2003)

[20] W. H. Baker, Is Information security under control?: Investigating quality in information security management, *IEEE Security & Privacy*, 5(1), 2007, 36-44.

[21] T. L. Saaty, The analytic hierarchy process: planning. Priority Setting. Resource Allocation, *(MacGraw-Hill, New York International Book Company*, 1980).

[22] E. Ngai, Selection of web sites for online advertising using the AHP, *Information & Management*, 40(4), 2003, 233-242.

[23] H. D. Wu, Systemic determinants of international news coverage: A comparison of 38 countries, *Journal of Communication*, 20(2), 2000, 110-130.

[24] P. Van Laarhoven, and W. A. Pedrycz, Fuzzy extension of Saaty's priority theory, Fuzzy sets and Systems, 11(1-3), 1983, 229-241.

[25] H. Gangwar, H. Date, and A. Raoot, Review on IT adoption: insights from recent technologies, *Journal of Enterprise Information Management*, 27(4), 2014, 488-502.

[26] A. Jeyaraj, J. Rottman, and M. Lacity, A review of the predictors, linkages, and biases in IT innovation adoption research, *Journal of Information Technology*, 12(1), 2006, 1-23.

[27] M. Kamal, IT innovation adoption in the government sector: identifying the critical success factors, *Journal Enterprise Information Management*, 19(2), 2006, 192-222.

[28] S. Al-Natour, and I. Benbasat, I. The adoption and IT artefacts: a new interaction-centric model for the study of user artefact relationships, *Journal of Association for Information Systems*, 10(9), 2009, 661-685.

[29] M. Hossain, and M. Quaddus, The adoption and continued usage intention of RFID: an integrated framework, *Information Technology & People*, 24(3), 2011, 236-256.

[30] I. Ajzen, The theory of planned behaviour, Organizational Behaviour and Human Decision Processes, 20(2), 1991, 179-211.

[31] E. Alsene, ERP systems and the co-ordination of the enterprise, *Business Process Management Journal*, 13(3), 2007, 417-432.

[32] E. Grandon, and J. Pearson, J. Electronic commerce adoption: an empirical study of small and medium US businesses, *Information and Management*, 42(1), 2004, 197-216.

[33] F. Davis, Perceived usefulness, perceived ease of use and acceptance of information technology, *MIS Quarterly*, 3(3), 1989, 319-340.

[34] M. Caldeira, and J. Ward, Understanding the successful adoption and use of IS/IT in SMEs: an explanation from Portuguese manufacturing industries, *Information Systems Journal*, 12(2), 2002, 121-152.

[35] S. Eze, H. Awa, J. Okoye, B. Emecheta, and R. Anazodo, Determinant factors of information communication technology (ICT) adoption by government-owned universities in Nigeria: a qualitative approach, *Journal of Enterprise Information Management*, 26(4), 2013, 427-443.